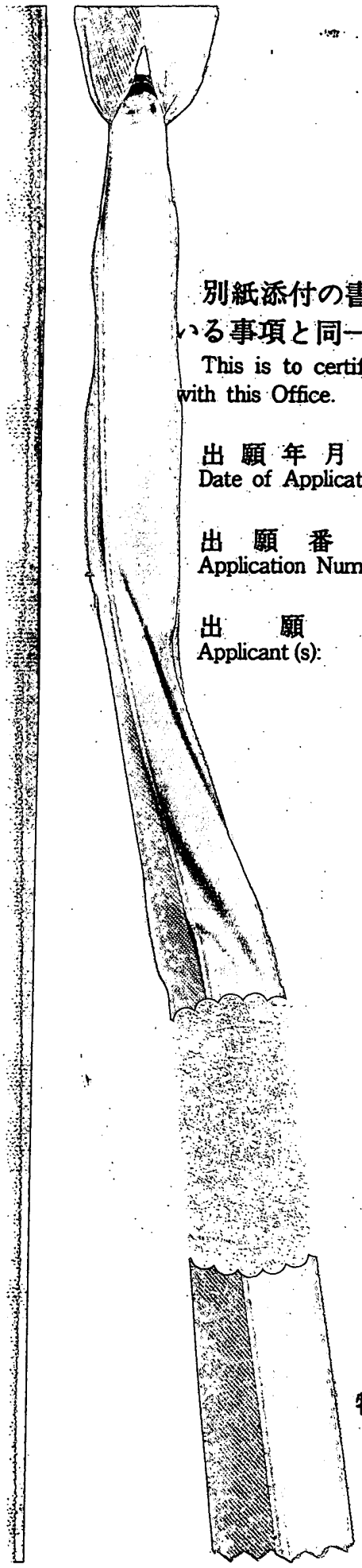
INOUE et al
040301|0539



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９７年 ９月 ５日

出 願 番 号
Application Number: 平成 ９年特許願第２４１１６７号

出 願 人
Applicant (s): 株式会社東芝

CERTIFIED COPY OF PRIORITY DOCUMENT

１９９８年 ４月１７日

特 許 庁 長 官
Commissioner,
Patent Office

荒井寿光

【書類名】　特許願

【整理番号】　A009704680

【提出日】　平成 9年 9月 5日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

【発明の名称】　移動計算機装置、読出制御方法及びメッセージ送出制御方法

【請求項の数】　12

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　井上　淳

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　石山　政浩

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　福本　淳

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　津田　悦幸

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　岡本　利夫

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　移動計算機装置、読出制御方法及びメッセージ送出制御方法

【特許請求の範囲】

【請求項１】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、

前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用い、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置宛てに、現在位置アドレスを含む登録要求メッセージを送信する手段と、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、ユーザ認証に成功した場合にのみ、前記外部インタフェース手段を通じた前記外部記憶装置からの読み出しを可能にする手段とを備えたことを特徴とする移動計算機装置。

【請求項２】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、

前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、ユ

ーザ認証に成功した場合にのみ、前記登録要求メッセージの送出を可能にする手段とを備えたことを特徴とする移動計算機装置。

【請求項３】

前記外部記憶装置に格納された前記ユーザ情報には、前記移動計算機を使用するユーザの個人情報が含まれ、

自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、前記外部記憶装置が自装置に接続した際にユーザ入力されたユーザ認証情報とが一致した場合に、ユーザ認証に成功したものと判断することを特徴とする請求項１または２に記載の移動計算機装置。

【請求項４】

自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、ユーザ入力されたユーザ認証情報とが一致しなかったことが、予め規定された回数連続して発生した場合には、それ以降の前記外部記憶装置からのデータ読み出しを不可能とすることを特徴とする請求項１に記載の移動計算機装置。

【請求項５】

自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、ユーザ入力されたユーザ認証情報とが一致しなかったことが、予め規定された回数連続して発生した場合には、それ以降の自装置からのメッセージの送出を不可能とすることを特徴とする請求項１に記載の移動計算機装置。

【請求項６】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、

前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネ

ットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、

前記登録要求メッセージの送受信を契機として行われる自装置と移動計算機管理装置との間のユーザ認証に、予め規定された回数連続して失敗した場合には、それ以降の前記外部記憶装置からのデータ読み出しを不可能とする手段とを備えたことを特徴とする移動計算機装置。

【請求項７】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、

前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、

前記登録要求メッセージの送受信を契機として行われる自装置と移動計算機管理装置との間のユーザ認証に、予め規定された回数連続して失敗した場合には、それ以降の自装置からのメッセージの送出を不可能とする手段とを備えたことを特徴とする移動計算機装置。

【請求項８】

前記外部記憶装置に格納される前記ネットワーク情報は、対象する移動計算機の移動前に所属するネットワークにおけるアドレス情報、前記移動計算機管理装置のアドレス情報および該移動計算機管理装置との間の認証のための情報のうちの少なくとも１つを含むものであることを特徴とする請求項１ないし７のいずれか１項に記載の移動計算機装置。

【請求項９】

前記外部記憶装置には対象とする移動計算機が移動先から暗号化処理を行って

通信を行う際に該移動計算機から発信した暗号化パケットを処理できるパケット中継装置のためのセキュリティ情報がさらに格納され、

前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記セキュリティ情報を用いて、移動先からの暗号化通信を行うことを特徴とする請求項１に記載の移動計算機装置。

【請求項１０】

前記外部記憶装置から読み出した情報を用いた通信が終了した際に、前記外部記憶装置から読み出した情報を、自装置の持つ記憶装置上から消去することを特徴とする請求項１に記載の移動計算機装置。

【請求項１１】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における読出制御方法であって、

ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置が自装置に接続されたことを契機として、ユーザにユーザ認証のための情報の入力を要求し、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、

このユーザ認証に成功した場合にのみ、前記外部記憶装置からの読み出しを可能にすることを特徴とする読出制御方法。

【請求項１２】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置におけるメッセージ送出制御方法であって、

ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置が自装置に接続されたことを契機として、ユーザにユーザ認証のための情報の入力を要求し、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、

このユーザ認証に成功した場合にのみ、前記外部記憶装置から読み出したネットワーク情報を用いて行うメッセージの送出を可能にすることを特徴とするメッセージ送出制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、相互接続している複数のネットワーク間で相互にデータを交換し必要なサービスを提供する複数の計算機により構成されるシステムにおける、ネットワーク間を移動して通信を行うことが可能な移動計算機装置、読出制御方法及びメッセージ送出制御方法に関する。

【０００２】

【従来の技術】

計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】

また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上を管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】

一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計

算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のＩＰパケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図１では、元々ホームネットワーク１ａに属していた移動計算機２が、他のネットワーク１ｂに移動し、ネットワーク１ｃ内の他の計算機（ＣＨ）３との間で通信を行う場合に、移動計算機２に対しホームエージェント（ＨＡ）５が上記の役割を行う。この方式は、インターネットの標準化団体であるＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＲＦＣ２００２，　ＩＰ　ｍｏｂｉｌｉｔｙ　ｓｕｐｐｏｒｔ　（Ｃ．Ｐｅｒｋｉｎｓ））。

【０００５】

ところで、移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。移動計算機への成り済ましなどの攻撃を回避するため、位置登録メッセージには移動計算機とホームエージェント間で予め交換したセキュリティ情報に従って認証コードが付加される。正しい認証コードが付加された登録メッセージでないと、移動計算機に位置登録は行われない。

【０００６】

しかしながら、移動ＩＰで規定されているセキュリティ対策はあくまでホスト（移動計算機）単位のセキュリティであり、その移動計算機を使用しているユーザの実体を認証するものではない。すなわち、例えば移動計算機にホスト間の認証のためのセキュリティ情報が保持されたまま、不正なユーザにホスト自体が盗まれると、不正なユーザが移動計算機に成り済まして、ホームネットワークの情報を取り出すことができ非常に危険である。

【０００７】

また、ホストを盗まれなくても、正規ユーザが登録処理までを行った移動計算

機を一時的に借用するだけで、ホームネットワーク上の機密情報を取り出されてしまうことも考えられる。

【０００８】

また、移動計算機を盗難された場合、移動計算機上に登録されている、ホームネットワークの情報（例えば、ホームエージェントのＩＰアドレスや、その認証用鍵、デフォルトルータや内部ホストのアドレスなど）も一緒に盗まれることになり、このような情報を元に別の攻撃を誘発する危険もある。すなわち、このような内部ネットワーク情報を推測させ得る情報については、できる限り移動計算機上に置かない方がセキュリティ的に望ましい。

【０００９】

すなわち、従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱いといえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。また、移動計算機が盗難された場合に、その上に登録されている内部ネットワーク情報なども併せて盗まれてしまうことになり、セキュリティ的に非常に危険な状況になる。

【００１０】

【発明が解決しようとする課題】

従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱く、移動先（外部ネットワーク）で内部ネットワークの機密情報が取り出されてしまうおそれがあった。また、移動計算機自身が盗難される場合を考えると、移動計算機上に登録されている、ホームネットワーク情報（例えば、ホームエージェントのＩＰアドレスや、その認証用鍵、デフォルトルータや内部ホストのアドレスなど）も一緒に盗まれることになり、このような情報を元に別の攻撃を誘発する危険もある。すなわち、このような内部ネットワーク情報を推測させ得る情報については、できる限り移動計算機上に置かない方がセキュリティ的に望ましい。

【００１１】

本発明は、上記事情を考慮してなされたもので、移動計算機にて用いるユーザ情報やネットワーク情報を不正に取得されることや、また不正に移動計算機を使用してそのホームネットワークに入り込むことを防止することの可能な移動計算機装置、読出制御方法及びメッセージ送出制御方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】

本発明（請求項１）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用い、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置宛てに、現在位置アドレスを含む登録要求メッセージを送信する手段と、前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、ユーザ認証に成功した場合にのみ、前記外部インタフェース手段を通じた前記外部記憶装置からの読み出しを可能にする手段とを備えたことを特徴とする。

【００１３】

本発明（請求項２）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、ユーザ認証に成功した場合にのみ、前記登録要求メッセージの送出を可能にする手段とを備えたことを特徴とする。

【0014】

好ましくは、前記外部記憶装置に格納された前記ユーザ情報には、前記移動計算機を使用するユーザの個人情報が含まれ、自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、前記外部記憶装置が自装置に接続した際にユーザ入力されたユーザ認証情報とが一致した場合に、ユーザ認証に成功したものと判断するようにしてもよい。

【0015】

好ましくは、自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、ユーザ入力されたユーザ認証情報とが一致しなかったことが、予め規定された回数連続して発生した場合には、それ以降の前記外部記憶装置からのデータ読み出しを不可能とするようにしてもよい。

【0016】

好ましくは、自装置に接続された前記外部記憶手段に格納された前記個人情報に対応して自装置内に記憶されているユーザ認証情報と、ユーザ入力されたユーザ認証情報とが一致しなかったことが、予め規定された回数連続して発生した場合には、それ以降の自装置からのメッセージの送出を不可能とするようにしてもよい。

【0017】

本発明（請求項6）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、前記登録要求メッセージの送受信を契機として行われる自装置と移動計算機管理装置との間のユーザ認証に、予め規定された回数連続して失敗した場合には、それ以降の前

記外部記憶装置からのデータ読み出しを不可能とする手段とを備えたことを特徴とする。

【００１８】

本発明（請求項７）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置に接続された、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から所望の情報を読み出す外部インタフェース手段と、前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記ネットワーク情報を用いて生成した、自装置に対するパケット転送サービスを提供する移動計算機管理装置に現在位置アドレスを含む登録要求メッセージを送信する手段と、前記登録要求メッセージの送受信を契機として行われる自装置と移動計算機管理装置との間のユーザ認証に、予め規定された回数連続して失敗した場合には、それ以降の自装置からのメッセージの送出を不可能とする手段とを備えたことを特徴とする。

【００１９】

好ましくは、前記外部記憶装置に格納される前記ネットワーク情報は、対象する移動計算機の移動前に所属するネットワークにおけるアドレス情報、前記移動計算機管理装置のアドレス情報および該移動計算機管理装置との間の認証のための情報のうちの少なくとも１つを含むものであってもよい。

【００２０】

好ましくは、前記外部記憶装置には対象とする移動計算機が移動先から暗号化処理を行って通信を行う際に該移動計算機から発信した暗号化パケットを処理できるパケット中継装置のためのセキュリティ情報がさらに格納され、前記外部インタフェース手段を通じて前記外部記憶装置から読み出した前記セキュリティ情報を用いて、移動先からの暗号化通信を行うようにしてもよい。

【００２１】

好ましくは、前記外部記憶装置から読み出した情報を用いた通信が終了した際に、前記外部記憶装置から読み出した情報を、自装置の持つ記憶装置上から消去するようにしてもよい。

【００２２】

本発明（請求項１１）は、

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における読出制御方法であって、

ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置が自装置に接続されたことを契機として、ユーザにユーザ認証のための情報の入力を要求し、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、

このユーザ認証に成功した場合にのみ、前記外部記憶装置からの読み出しを可能にすることを特徴とする読出制御方法。

【００２３】

本発明（請求項１２）は、

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置におけるメッセージ送出制御方法であって、

ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置が自装置に接続されたことを契機として、ユーザにユーザ認証のための情報の入力を要求し、

前記ユーザ情報およびユーザ入力された情報に基づいたユーザ認証を行い、

このユーザ認証に成功した場合にのみ、前記外部記憶装置から読み出したネットワーク情報を用いて行うメッセージの送出を可能にすることを特徴とするメッセージ送出制御方法。

【００２４】

なお、以上の各装置に係る発明は方法に係る発明としても成立し、方法に係る発明は装置に係る発明としても成立する。

また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００２５】

従来、移動ＩＰ方式では、ホスト単位の認証により、移動ホストへの成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますというユーザ成

り済まし攻撃には対応されていない。そのため、移動先（外部ネットワーク）から内部ネットワークの機密情報が不正に取り出されてしまうおそれがあった。また、移動計算機自身が盗難される場合を考えると、移動計算機上に登録されている、ネットワーク情報（例えば、ホームエージェントのＩＰアドレスや、その証明用鍵、デフォルトルータや内部ホストのアドレスなど）も一緒に盗まれることになり、このような情報を元に別の攻撃を誘発する危険もある。すなわち、このような内部ネットワーク情報を推測され得る情報については、できる限る移動計算機上に置かない方がセキュリティ的に望ましい。

【００２６】

本発明によれば、ユーザ情報やネットワーク情報は移動計算機内ではなく外部記憶装置に格納してユーザが携帯し、これを必要時に移動計算機に装着し、外部記憶装置から必要な情報を移動計算機内に読み込み、現在位置登録メッセージの送信やネットワーク情報の構成等を行うことができるので、ユーザ情報やネットワーク情報の記憶されていない移動計算機のみでは情報の漏洩も移動計算機からホームネットワークへの通信も行うことはできない。

【００２７】

また、外部記憶装置から移動計算機への情報の読み込みを、ユーザ認証に成功した場合にのみ可能とするように制御を行えば、ユーザ認証を成功させることのできない不正ユーザは、外部記憶装置から情報を取得することもホームネットワークへの通信を行うこともできない。

【００２８】

また、外部記憶装置から移動計算機へ読み込んだ情報を用いた移動計算機からのメッセージの送出を、ユーザ認証に成功した場合にのみ可能とするように制御を行うので、ユーザ認証を成功させることのできない不正ユーザは、少なくともホームネットワークへの通信を行うことはできない。

【００２９】

また、一定回数ユーザ認証に失敗した場合には、それ以降の外部記憶装置から移動計算機への情報の読み込み、あるいは外部記憶装置から移動計算機へ読み込んだ情報を用いた移動計算機からのメッセージの送出を、不可能とするように制

御を行えば、より優れたセキュリティを得ることができる。

また、一切の機密情報を移動計算機上に残さないことで、移動計算機自身が盗難された場合も内部情報の盗難を防止することができる。

【００３０】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

（１）図１に、本実施形態に係る通信システムの基本構成の一例を示す。

図１の通信システムは、移動ＩＰ（ＲＦＣ２００２）により移動計算機の通信をサポートしているものとする。なお、移動ＩＰプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動計算機自身がフォーリンエージェントを兼ねる）Ｃｏ－ｌｏｃａｔｅｄ　Ｃａｒｅ－ｏｆ　ａｄｄｒｅｓｓモードがあるが、本実施形態では、後者を採用するものとして説明する。

【００３１】

図１では、ホームネットワーク１ａ、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃがインターネット６を介して相互に接続されており、移動計算機（ＭＮ）２、移動計算機の通信相手（ＣＨ）３は、これらネットワーク内に接続され、または外部ノードとしてインターネット６に接続される。

【００３２】

本実施形態では、ネットワーク１ａの内部をホームポジションとする移動計算機２が他部署ネットワーク１ｂに移動した場合について説明する。

ホームネットワーク１ａには、移動ＩＰプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント（ＨＡ）５が設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機２宛に転送されてきたＩＰパケットは、そのホームエージェント５を経由し、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化することで、移動計算機２に対するデータの経路制御を行うことができ

る。

【0033】

移動計算機2は、自装置がホームネットワーク外に移動した場合には、移動先のネットワーク（ここでは1b）において、例えばDHCPやPPPなどのプロトコルにより移動先ネットワークで使用するアドレスを獲得する。アドレスを獲得したら、移動計算機2は、ホームネットワーク1aのホームエージェント5に現在位置の情報を含む登録メッセージを送信する。

【0034】

図2に移動計算機2からホームエージェント5に送信される登録メッセージの形式を示す。

フラグ（FLAG）は移動IPの動作モード（カプセル化の方法など）を示す。

【0035】

Lifetimeは、この登録の有効期限を示す。移動計算機2は有効期限を越えた場合、再度登録メッセージをホームエージェント5に送信し、再登録を行わなくてはいけない。

【0036】

Home Addressは移動計算機のホーム位置を、Care-of Addressは移動計算機の現在位置を、Home Agentはホームエージェント5のアドレスを示す。

【0037】

Identificationは登録に対するIDでリプレイ攻撃を防止するために付加される。

Extensionsには少なくとも移動計算機2～ホームエージェント5間のホスト認証のためのホスト認証情報が含まれる。

【0038】

図3に、本実施形態に係る移動計算機システムの要部構成の一例を示す。本実施形態では、移動通信に必要な情報は移動計算機2本体内には保持せず、外部記憶装置12内に保持するようにしている。ここでは、外部記憶装置12の中には

ユーザ情報１２１、ホームエージェント情報１２２、ホームアドレス情報１２３を保持するものとする。外部記憶装置１２としては、例えばメモリカード３１を使用することができる。

【００３９】

必要に応じて外部記憶装置１２を接続された移動計算機２はそのインタフェース２１を介して、この外部記憶装置１２からユーザ情報１２１、ホームエージェント情報１２２、ホームアドレス情報１２３を取り出し、これらの情報をもとに図２に例示する登録メッセージをメッセージ生成部２２にて構成し、ホームエージェント５に宛てて送出する。他のデータの通信で外部記憶装置１２内の情報を必要とする場合も上記と同様である。

【００４０】

本実施形態では、例えば移動計算機２が自装置に外部記憶装置１２が装着されたことを検出した際に（あるいは既に外部記憶装置１２が装着されている移動計算機２が起動された際に、あるいは特定の通信プログラムが起動した際に）、移動計算機２は、自装置内に記憶されているユーザ個人情報（例えばユーザＩＤ）とパスワードの組のうち、装着された外部記憶装置１２から読み出したユーザ情報１２３に含まれるユーザ個人情報に対応するパスワードをユーザに入力要求する（上記組は１組としユーザが予めパスワードを設定しておいてもよい）。これにより例えば紛失した外部記憶装置１２を他人が不正に使用することを防止することができる。

【００４１】

入力されたパスワードと移動計算機２内に設定されたユーザ情報１２３に対応するパスワードとの照合に成功すれば、外部記憶装置１２内に格納された情報が直ちにまたは必要時に移動計算機２内のディスクやＲＡＭなどの所定の記憶装置にロードされ、必要な通信に使用される。

【００４２】

パスワード認証に失敗した場合には、再度、ユーザにパスワードを入力要求するメッセージを呈示し、それでもなおパスワードを所定回数（１回の場合も含む）入力失敗した場合には、それ以降の外部記憶装置１２からの一切の情報読出し

をロックアウトするようにするのが好ましい。

【００４３】

なお、外部記憶装置１２から移動計算機２内にロードした情報は、この情報を必要とする通信プログラムが終了した時点で、あるいは移動計算機２の立ち下げにあたって、あるいは外部記憶装置１２が移動計算機２から抜き出された際に、当該移動計算機２内のディスクやＲＡＭなどの全ての記憶装置上から消去するのが望ましい（このデータ消去の契機の例と上記のパスワード入力の契機の例とは任意に組み合わせ可能である）。

【００４４】

なお、上記では、パスワード認証を外部記憶装置１２からのデータ読み込みの可／不可の制御に用いたが、その代わりに、パスワード認証に成功したら、メッセージの送出を可能とし、パスワード認証に一定回数連続して失敗した場合には、それ以降の自装置からの登録要求メッセージあるいは一切のメッセージ送出を不可とするような制御を行ってもよい。

【００４５】

また、上記のようにパスワード認証で外部記憶装置１２からのデータ読み込みの可／不可を制御するのに加えて、別のパスワードを用意し、これを登録要求送出の可／不可の制御に用いることも可能である。

【００４６】

（２）より安全に移動計算機２を使用することができるようにするために、移動計算機２とそのホームネットワークのホームエージェント５との間でユーザ認証を行う機能を付加すると好ましい。移動計算機２－ホームエージェント５間でのユーザ認証としては、移動計算機２がホームエージェント５に登録メッセージを送信する際にこの登録メッセージにユーザ認証のための情報を含める方法が考えられる。この場合、例えば外部記憶装置１２から読み込んだユーザ情報１２３の全部または一部を図２に例示した登録メッセージのＥｘｔｅｎｓｉｏｎの部分に適当な形式で組み込んで送信することにより、ホームエージェント５側でユーザ認証を行うことができる。このＥｘｔｅｎｓｉｏｎ部分に含ませるユーザ情報（Ｕｓｅｒ　ｉｎｆｏ）のデータ形式の一例を図４に示す。

【0047】

このような登録要求メッセージを移動計算機2からホームエージェント5に送信すると、ホームエージェント5は、まず、ホスト認証情報を調べホスト認証を行うとともに、ユーザ情報を調べユーザ認証を行う。そして、ホスト認証とユーザ認証の両方に成功しならば、ホームエージェント5は、移動計算機2の現在位置の登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置を登録して移動計算機2へのデータパケットの転送を開始する。なお、少なくとも一方の認証が失敗したならば、例えばホスト認証および／またはユーザ認証に失敗した旨の情報を含む登録失敗メッセージを移動計算機2に返送する。

【0048】

（3）上記の（2）とは別の移動計算機2－ホームエージェント5間でのユーザ認証として次のような機能を付加すると好ましい。移動計算機2が盗難されるような場合を想定すると、不正ユーザが使用できないようにユーザパスワード要求をホームエージェントから返す方法が望ましい。この場合、ホームエージェント5が、移動計算機2からの登録メッセージを受信すると、移動計算機2との間でのユーザ認証手順の実行を起動し、ユーザ認証に成功したことを条件に登録の処理を行うようにする方法が考えられる。

【0049】

例えば図5のようにホームエージェント5が移動計算機2を使用しているユーザを認証するため、チャレンジ～レスポンスによるメッセージを交換するものが考えられる。なお、チャレンジメッセージの形式を図6（a）に、レスポンスメッセージの形式を図6（b）に示す。

【0050】

この例では、移動計算機2が登録要求メッセージをホームエージェント5に送信すると、ホームエージェント5は、まず、認証情報を調べホスト認証を行う。そして、ホスト認証に成功しならばホームエージェント5はチャレンジメッセージを移動計算機2に返信する。

【0051】

移動計算機２は、このチャレンジメッセージを受けると、ユーザの入力した認証データを含むレスポンスメッセージを、ホームエージェント５に送信する。なお、認証データは例えばパスワードである。また、このパスワードとしては、上記した（１）におけるパスワードと同じものを用いる方法と、別のものを用いる方法がある。

【００５２】

レスポンスメッセージを受け取ったホームエージェント５は、レスポンスメッセージに含まれる認証データと、予めホームネットワーク駐在時に該移動計算機に対応して登録してあったものとを比較して、受け取った認証データが正しいか否かを調べ、その結果、該移動計算機２から返された認証データが正しいものであることが確認されたならば、現在位置の登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置を登録して移動計算機２へのデータパケットの転送を開始する。

【００５３】

なお、ホームエージェント５は、認証データが正しいものでないと判断した場合、移動計算機２に、ユーザ認証に失敗した旨のメッセージを送信して一連の手順を中止するか、あるいはユーザ認証に失敗した旨の情報を含む再度のチャレンジメッセージを送信するものとする。また、後者の場合、このメッセージ交換を規定回数繰り返しても正しい認証データが送信されてこなかった場合には、一連の手続きを中止し、ユーザ認証に失敗した旨を示すメッセージを返すのが好ましい。

【００５４】

なお、上記では、パスワードのやり取りを行う例を示したが、ホームエージェント５から渡されたその都度生成される第１のデータと、ユーザが入力した第２のデータとから、外部記憶装置１２内（または移動計算機２本体内）に格納されている所定の関数を用いて、ワンタイムパスワードを生成し、これを移動計算機２からホームエージェント５へ返し、ホームエージェント５では、自身が生成した第１のデータと、予め記憶しておいた第２のデータと所定の関数とをもとに、返されたワンタイムパスワードが正しいか否かを調べるようにしてもよい。

【００５５】

（４）上記の（３）においては、不正ユーザが正しくないデータを入力するなどして移動計算機２が一定回数以上のユーザ認証レスポンス失敗を繰り返した場合、それ以降は外部記憶装置１２からのデータ読み出しを不可能とする機能を付加するのが好ましい。そのような例を図７および図８を参照しながら説明する。図７はこの場合に移動計算機２に付加する機能を示すブロック図の一例であり、図８はその手順の一例である。

【００５６】

図７の機能を持つ移動計算機２において、予めユーザ（システム管理者あるいは移動計算機の使用者等）が指定する連続ユーザ認証失敗回数を移動計算機２内の失敗回数レジスタ２３に入力する（ステップＳ１１）。

【００５７】

移動計算機２がユーザ認証に失敗した旨のメッセージをホームエージェント５から受信する毎に、（予め初期化しておいた）認証失敗回数カウンタ２４をインクリメントする（ステップＳ１２～Ｓ１５）。一方、ユーザ認証に成功したら（ステップＳ１３でＹｅｓの場合）、認証失敗回数カウンタ２４は０にリセットされる。

【００５８】

しかして、ステップＳ１５において、比較部２５にてレジスタ２３と認証失敗回数カウンタ２４の値を比較して、それらが一致したら（ステップＳ１５でＹｅｓの場合）、移動計算機２はデータ読み出し禁止制御部２６を起動し、これ以降の一切のデータ読み出しを停止する（ステップＳ１６）。

【００５９】

上記のように所定回数パスワード入力失敗を繰り返し、それ以降はデータ読み出し禁止制御部２６により外部記憶装置１２からのデータ読み出しを不可能とした場合、このデータ読み出し禁止を解除するには、この移動計算機２に固有のホームエージェント内に格納されている情報を使用しなくてはいけないものとする。例えば、ホームエージェント５側で管理される、データ読み出し禁止制御部２６のデータ読み出し禁止を解除するためのユーザデータ（インストール時にシス

テム管理者が設定する）を、ＦＤなどオフライン機構で発行し、これを使用して移動計算機２側のロックを解除する。

【００６０】

なお、データ読み出し禁止制御部２６は外部記憶装置１２内に設け、ロック解除のためのユーザデータを特殊なメモリカードライタ（外部記憶装置１２がメモリカードの場合）等を使って書き込むことで、外部記憶装置１２内のデータ読み出し禁止制御部２６を解除するようにしてもよい。

【００６１】

（５）上記の（４）では規定回数ユーザ認証に失敗した場合に外部記憶装置１２のデータ読み出し禁止を行う例であったが、別の例として、規定回数ユーザ認証に失敗した場合に登録要求メッセージの送出を抑止するようにしてもよい。そのような例を図９および図１０を参照しながら説明する。図９はこの場合に移動計算機２に付加する機能を示すブロック図の一例であり、図１０はその手順の一例である。

【００６２】

図９の機能を持つ移動計算機２において、予めユーザ（システム管理者あるいは移動計算機の使用者等）が指定する連続ユーザ認証失敗回数を失敗回数レジスタ２７に入力する（ステップＳ２１）。

【００６３】

移動計算機２がユーザ認証に失敗した旨のメッセージをホームエージェント５から受信する毎に、（予め初期化しておいた）認証失敗回数カウンタ２８をインクリメントする（ステップＳ２２～Ｓ２５）。一方、ユーザ認証に成功したら（ステップＳ２３でＹｅｓの場合）、認証失敗回数カウンタ２８は０にリセットされる。

【００６４】

しかして、ステップＳ２５において、比較部２９にてレジスタ２７と認証失敗回数カウンタ２８の値を比較して、それらが一致したら（ステップＳ２５でＹｅｓの場合）、移動計算機２はメッセージ送出停止制御部３０を起動し、これ以降の一切のメッセージ送出を停止する（ステップＳ２６）。メッセージ送出停止制

御部３０によるメッセージ送信抑止を解除するには、この移動計算機２に固有のホームエージェント内に格納されている情報を使用しなくてはいけないものとする。

【００６５】

上記のように所定回数パスワード入力失敗を繰り返し、それ以降はメッセージ送出停止制御部３０によりメッセージ送信を不可能とした場合、このメッセージ送信抑止を解除するには、この移動計算機２に固有のホームエージェント内に格納されている情報を使用しなくてはいけないものとする。例えば、ホームエージェント５側で管理される、メッセージ送出停止制御部３０のメッセージ送出抑止を解除するためのユーザデータ（インストール時にシステム管理者が設定する）を、ＦＤなどオフライン機構で発行し、これを使用して移動計算機２側のロックを解除する。

【００６６】

（６）以下では、上記した（１）～（５）において、移動計算機２が、移動ＩＰと共にパケットの暗号化を行う場合に付加する機能について説明する。例えば、図１１に示すように、ホームネットワーク１ａや他部署ネットワーク１ｄには暗号通信機能を有するパケット暗号化ゲートウェイ装置４ａ，４ｄが存在し、移動計算機２が他部署ネットワーク１ｄ内にあるいは外部ノードとして接続され、移動計算機２とホームネットワーク１ａのゲートウェイ装置４ａとの間で暗号パラメータをやりとりし、途中を流れるパケットを暗号化することが考えられる。この場合も、ゲートウェイ装置４ａのアドレスや、そのセキュリティ情報（暗号化パラメータなど）は、（１）～（５）と同様に、移動計算機２本体内ではなく、メモリカード等の外部記憶装置１２内に格納しておき、これら情報を外部記憶装置１２から移動計算機２に取り出して必要な処理を行うことが考えられる。

【００６７】

図１２には、そのようなセキュリティ情報をも外部記憶装置１２から読み出すようにした場合の移動計算機システムの要部構成を示す。この場合、外部記憶装置１２内に、ユーザ情報１２１、ホームエージェント情報１２２、ホームアドレス情報１２３に加え、ゲートウェイアドレス１２４、セキュリティパラメータ１

２５をも記憶しておき、（１）～（５）で示したような手順で、インタフェース２１を介して読み出して、移動計算機２との間での暗号化通信に使用する。

【００６８】

なお、以上述べた実施形態において、外部記憶装置（例えばメモリカード）に記憶される情報は、ユーザ情報や、ネットワーク（アドレス）情報、セキュリティ情報など、外部に漏洩されたくない情報である。従って、メモリカードからの情報については必要な際にインタフェースを介して読み出すが、移動計算機２上に複製を作成しないように注意すべきである。

【００６９】

従来、移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の認証により、移動ホストへの成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますというユーザ成り済まし攻撃には対応されておらず、この攻撃には極めて弱い。そのため、移動先（外部ネットワーク）から内部ネットワークの機密情報が不正に取り出されてしまうおそれがあった。また、移動計算機自身が盗難される場合を考えると、移動計算機上に登録されている、ホームネットワーク情報（例えば、ホームエージェントのＩＰアドレスや、その証明用鍵、デフォルトルータや内部ホストのアドレスなど）も一緒に盗まれることになり、このような情報を元に別の攻撃を誘発する危険もある。すなわち、このような内部ネットワーク情報を推測され得る情報については、できる限る移動計算機上に置かない方がセキュリティ的に望ましい。

【００７０】

本実施形態によれば、ユーザ情報または携帯端末に関するネットワーク情報をを保持する外部記憶装置を用い、この外部記憶装置に記憶されている情報を元に、移動計算機の現在位置登録メッセージの送信や、ネットワーク情報の構成を行うことができる。また、一切の機密情報を移動計算機上に残さないことで、移動計算機自身が盗難された場合も内部情報の盗難を防止することができる。

【００７１】

なお、本実施形態では、Ｃｏ－ｌｃａｔｅｄ　Ｃａｒｅ－ｏｆ　Ａｄｄｒｅｓｓモードによる通信システムについて説明したが、本発明は、フォーリンエージ

ェントの存在を仮定した移動通信システムにも適用可能である。

【００７２】

また、本発明は、ＲＦＣ２００２に示される移動ＩＰだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。

また、以上の各機能、例えば処理の部分の他、移動計算機内のカウンタなどもハードウェアとしてもソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

【００７３】

なお、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００７４】

【発明の効果】

本発明によれば、ユーザ情報やネットワーク情報を移動計算機内ではなく外部記憶装置に格納し、これを必要時に移動計算機内に読み込みむようにするとともに、この外部記憶装置から移動計算機への情報の読み込みあるいは外部記憶装置から移動計算機へ読み込んだ情報を用いた移動計算機からのメッセージの送出をユーザ認証に成功した場合にのみ可能とするようにしたので、ユーザ認証を成功させることのできない不正ユーザは、外部記憶装置から情報を取得することやホームネットワークへの通信を行うことなど、ユーザ情報やネットワーク情報に関する不正操作をすることができず、優れたセキュリティを得ることができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係るネットワークの基本構成を示す図

【図２】

同実施形態に係る移動計算機の送信する登録要求メッセージ形式を示す図

【図３】

同実施形態に係る移動計算機の構成例を示す図

【図４】

同実施形態に係る移動計算機の送信するホスト認証のための拡張した登録要求メッセージを説明するための図

【図５】

ユーザ認証方式を説明するための図

【図６】

ユーザ認証のためのメッセージの形式の一例を示す図

【図７】

同実施形態に係る移動計算機の構成例を示す図

【図８】

図７の移動計算機の動作手順を示すフローチャート

【図９】

同実施形態に係る移動計算機の構成例を示す図

【図１０】

図９の移動計算機の動作手順を示すフローチャート

【図１１】

同実施形態に係るネットワークの他の基本構成を示す図

【図１２】

同実施形態に係る移動計算機の構成例を示す図

【符号の説明】

１ａ，１ｂ，１ｃ，１ｄ…ネットワーク

２…移動計算機、

３…通信相手計算機

４ａ，４ｄ…パケット暗号化ゲートウェイ装置

５…ホームエージェント

６…インターネット

１２…外部記憶装置

２１…インタフェース

２２…メッセージ生成部

２３…失敗回数レジスタ

２４…失敗回数カウンタ

２５…比較部

２６…データ読み出し禁止制御部

２７…失敗回数レジスタ

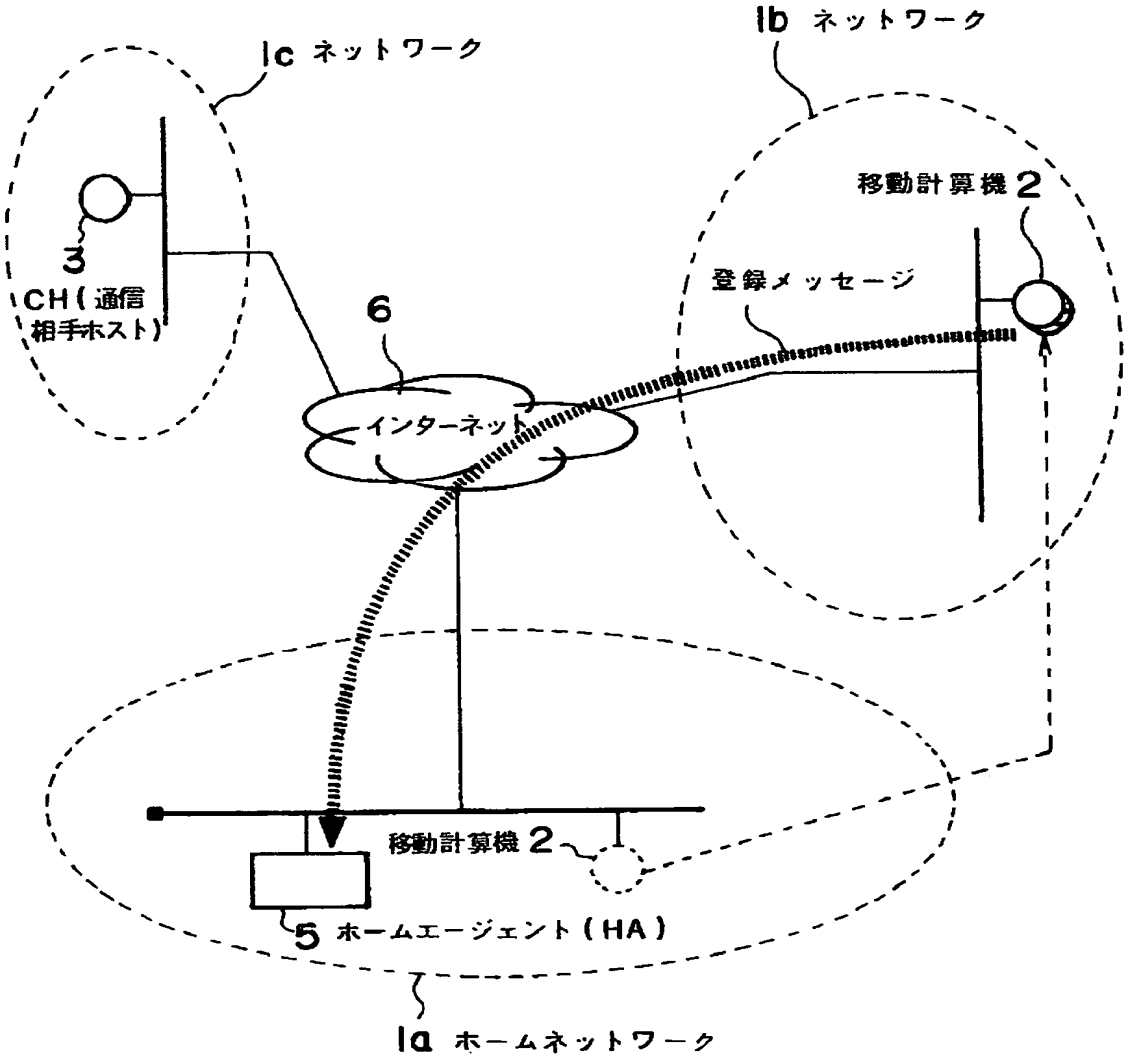
２８…失敗回数カウンタ

２９…比較部

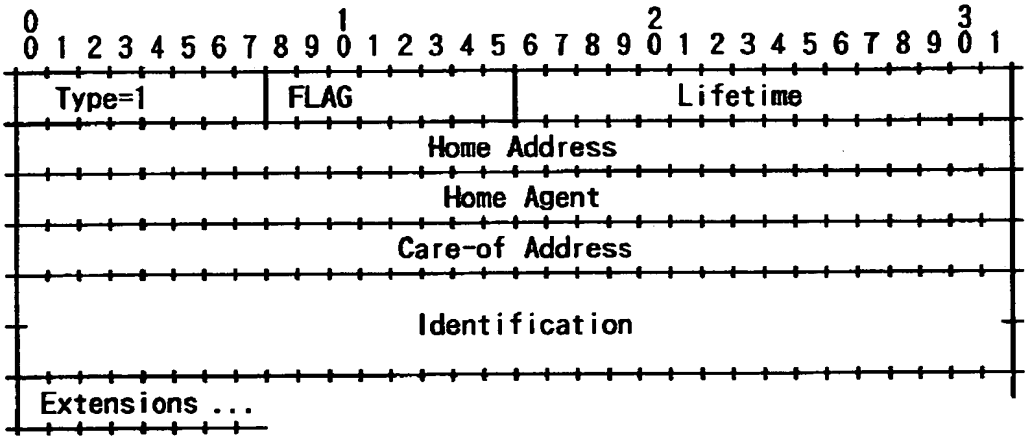
３０…メッセージ送出停止制御部

【書類名】　　図面

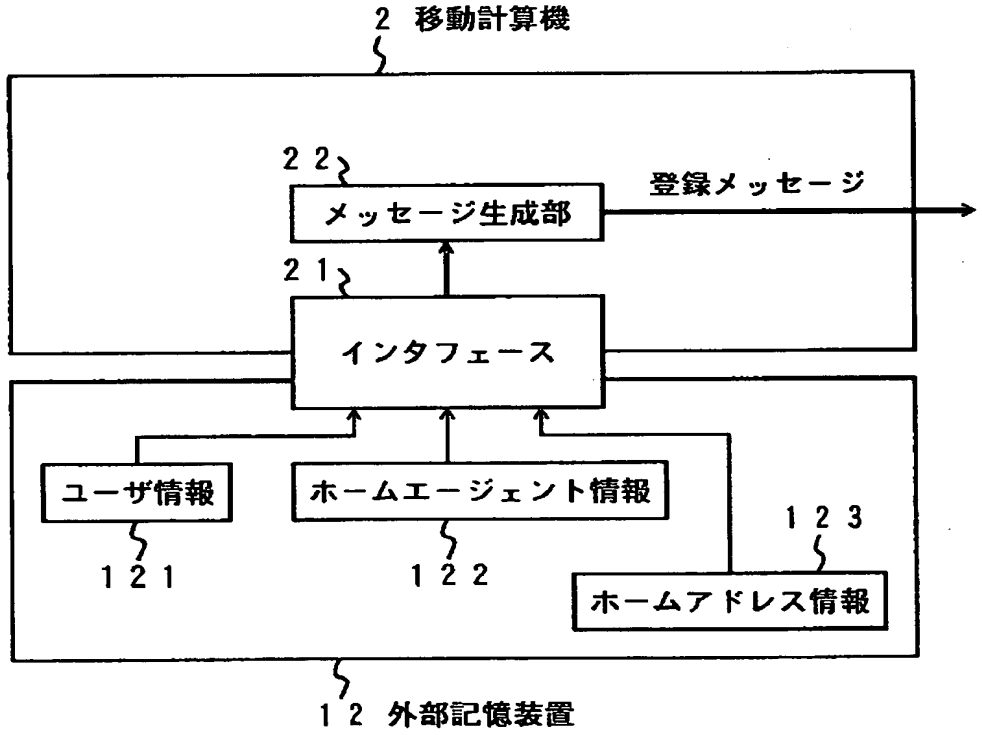
【図１】


1b ネットワーク
1c ネットワーク
移動計算機 2
3
CH（通信相手ホスト）
登録メッセージ
6
インターネット
移動計算機 2
5 ホームエージェント（HA）
1a ホームネットワーク

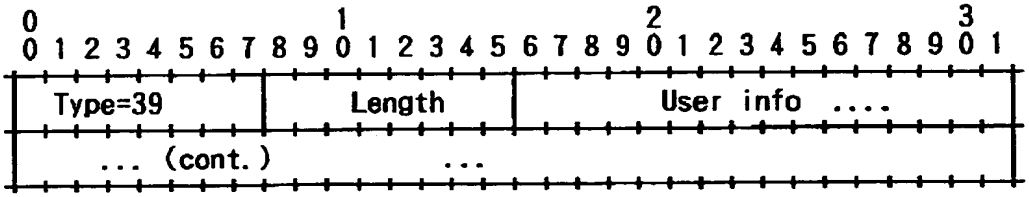
【図２】


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type=1
FLAG
Lifetime
Home Address
Home Agent
Care-of Address
Identification
Extensions ...

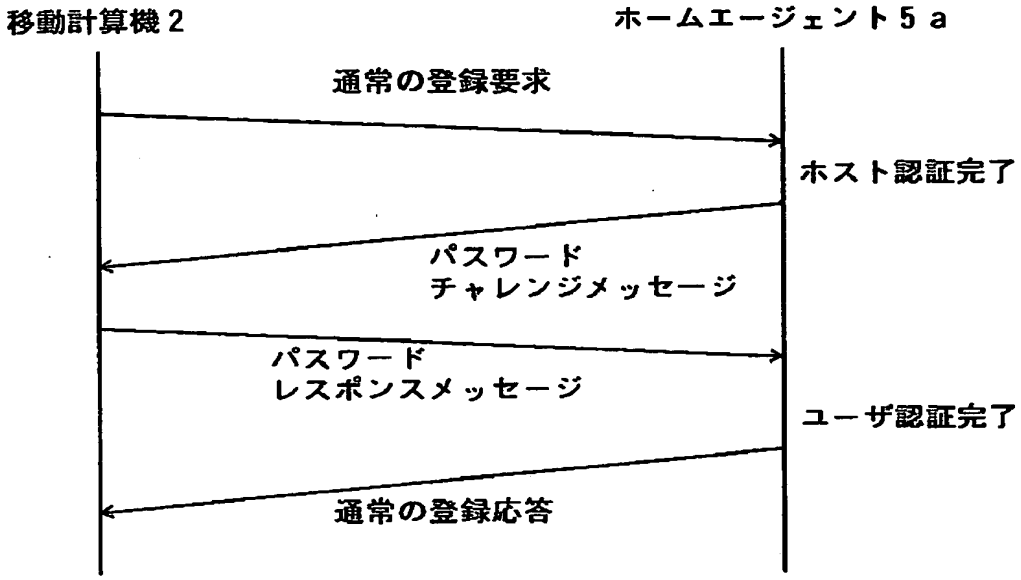
【図３】


2 移動計算機
22
メッセージ生成部
登録メッセージ
21
インタフェース
ユーザ情報
ホームエージェント情報
123
121
122
ホームアドレス情報
12 外部記憶装置

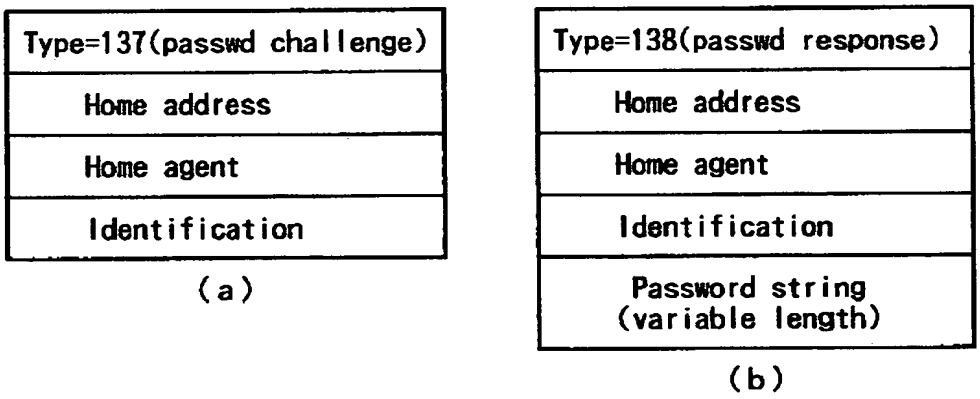
【図４】


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type=39
Length
User info ....
... (cont.)
...

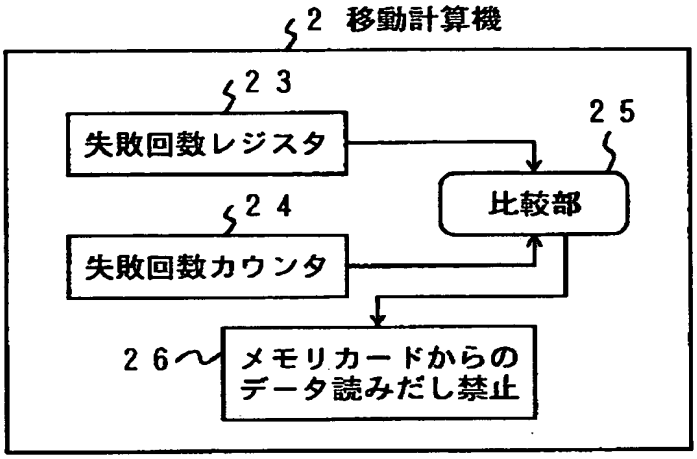
【図５】


移動計算機２
ホームエージェント５ａ
通常の登録要求
ホスト認証完了
パスワード
チャレンジメッセージ
パスワード
レスポンスメッセージ
ユーザ認証完了
通常の登録応答

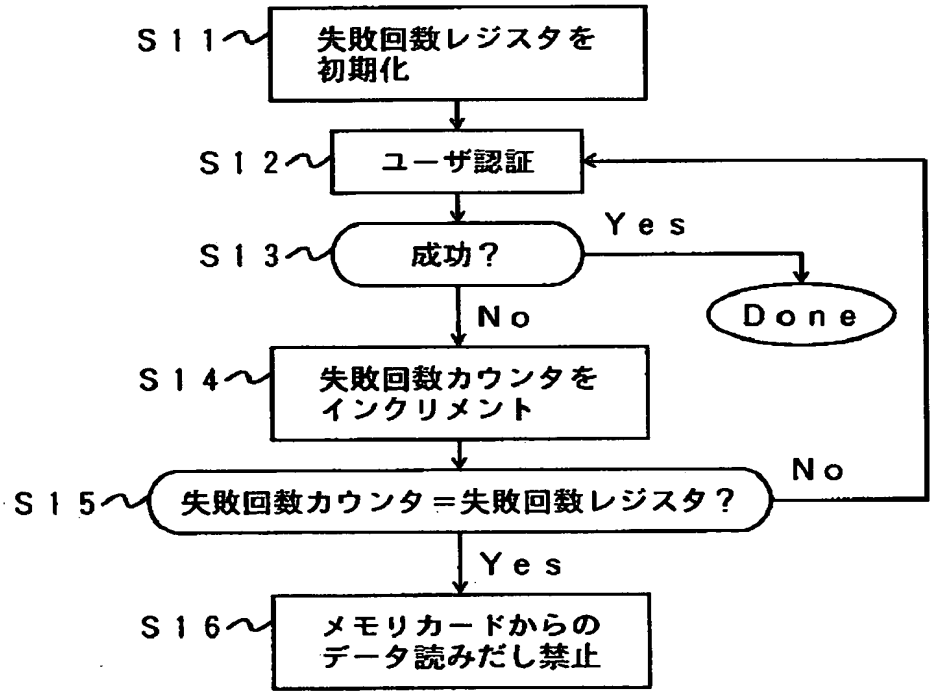
【図６】


Type=137(passwd challenge)
Home address
Home agent
Identification
(a)
Type=138(passwd response)
Home address
Home agent
Identification
Password string
(variable length)
(b)

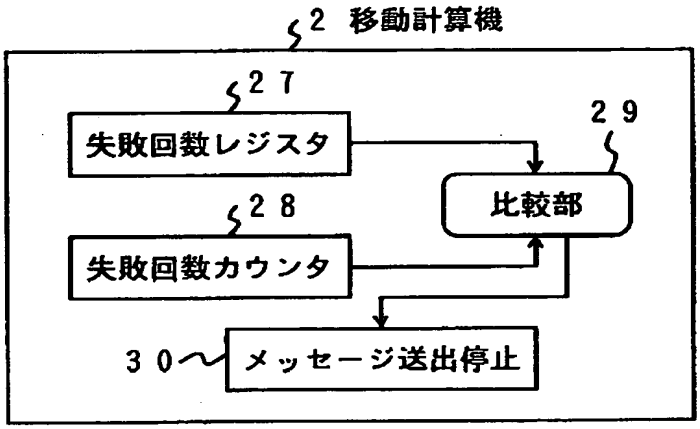
【図7】


2 移動計算機
23
失敗回数レジスタ
25
比較部
24
失敗回数カウンタ
26
メモリカードからの
データ読みだし禁止

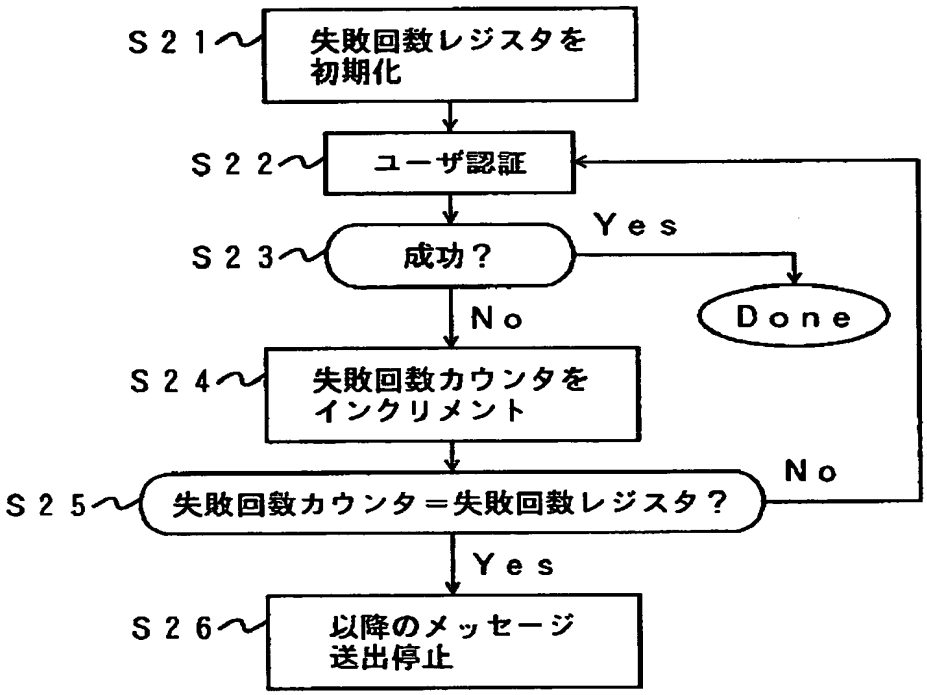
【図8】


S11
失敗回数レジスタを
初期化
S12
ユーザ認証
S13
成功？
Yes
Done
No
S14
失敗回数カウンタを
インクリメント
S15
失敗回数カウンタ＝失敗回数レジスタ？
No
Yes
S16
メモリカードからの
データ読みだし禁止

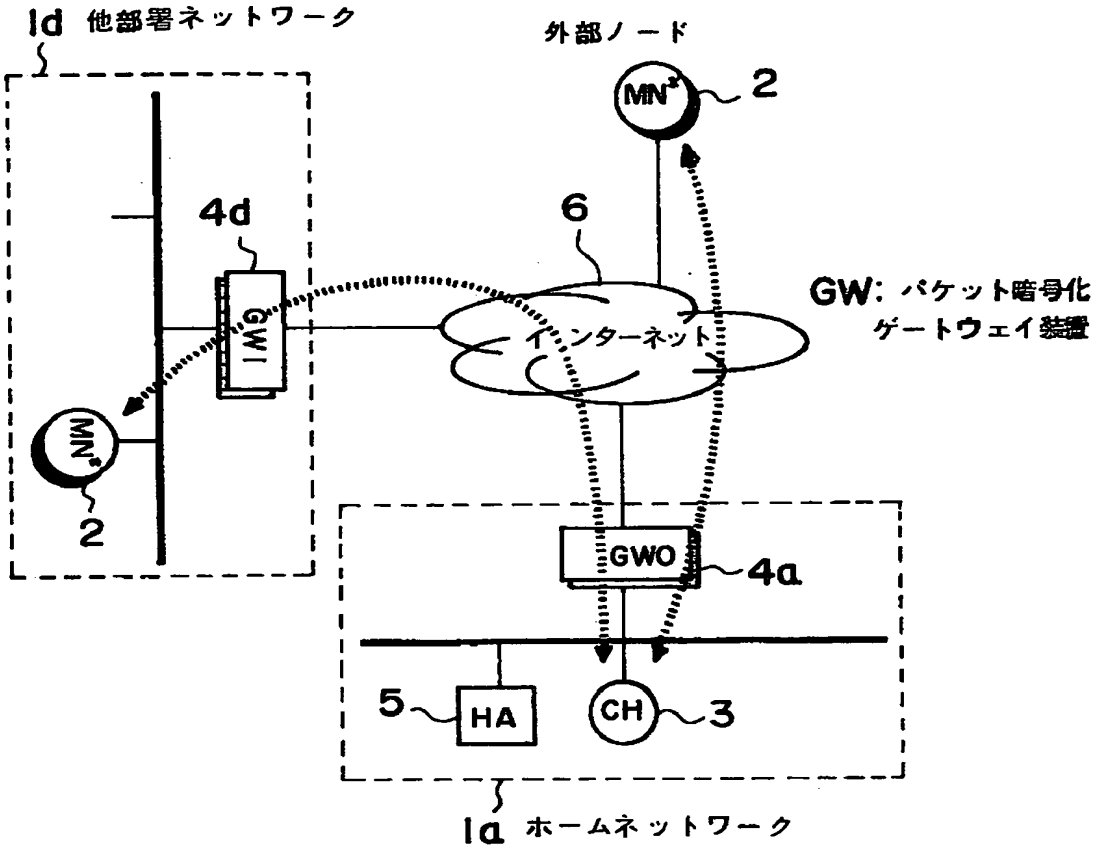
【図９】


2 移動計算機
27
失敗回数レジスタ
29
比較部
28
失敗回数カウンタ
30
メッセージ送出停止

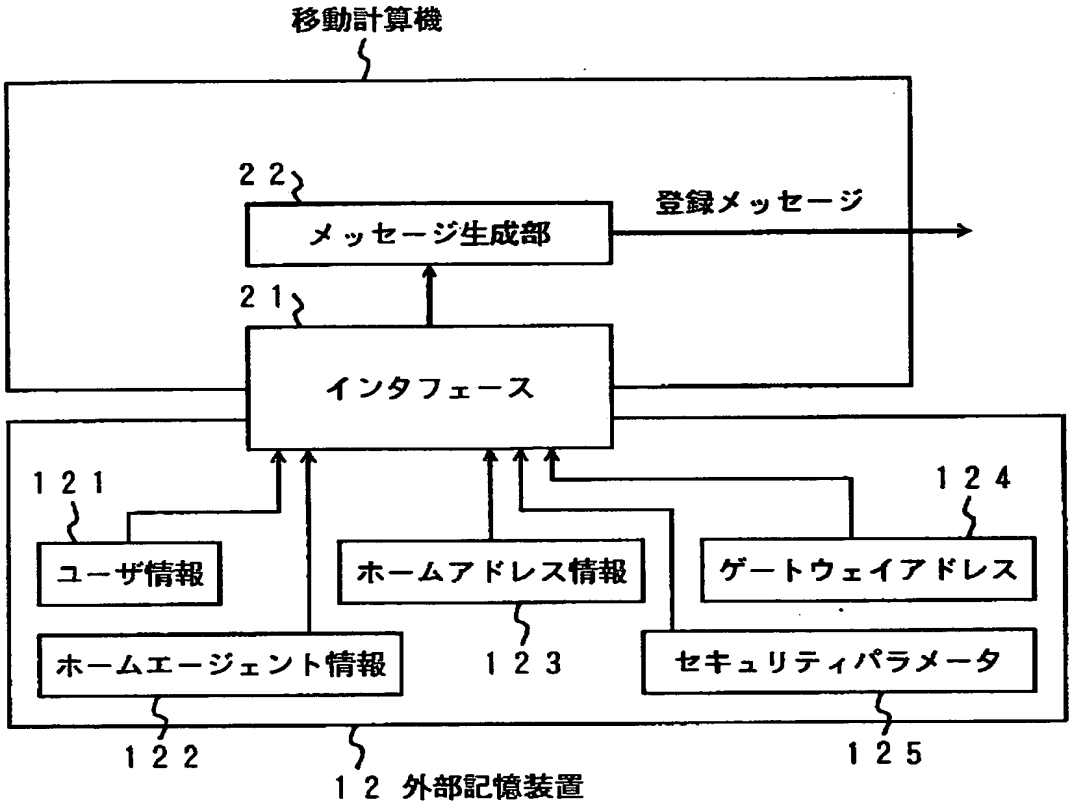
【図１０】


S21
失敗回数レジスタを初期化
S22
ユーザ認証
S23
成功？
Yes
Done
No
S24
失敗回数カウンタをインクリメント
S25
失敗回数カウンタ＝失敗回数レジスタ？
No
Yes
S26
以降のメッセージ送出停止

【図１１】


1d 他部署ネットワーク
外部ノード
MN
2
4d
6
GW1
インターネット
GW: パケット暗号化
ゲートウェイ装置
MN
2
GWO
4a
5
HA
CH
3
1a ホームネットワーク

【図１２】


移動計算機
２２
メッセージ生成部
登録メッセージ
２１
インタフェース
１２１
ユーザ情報
ホームアドレス情報
１２４
ゲートウェイアドレス
ホームエージェント情報
１２３
セキュリティパラメータ
１２２
１２５
１２　外部記憶装置

【書類名】　　要約書

【要約】

【課題】　移動計算機にて用いるユーザ情報やネットワーク情報を不正に取得されることや不正に移動計算機を使用してそのホームネットワークに入り込むことを防止することの可能な移動計算機を提供すること。

【解決手段】　相互接続されたネットワーク間を移動して通信可能な移動計算機であって、ユーザ情報および移動先での通信に用いるネットワーク情報を少なくとも格納している外部記憶装置から情報を読出す外部インタフェース（Ｉ／Ｆ）と、Ｉ／Ｆを通じて外部記憶装置から読出したネットワーク情報を用い、自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置宛てに、現在位置アドレスを含む登録要求メッセージを送信する送信部を備え、ユーザ情報およびユーザ入力された情報に基づいたユーザ認証に成功した場合にのみ外部インタフェースを通じた外部記憶装置からの読出しを可能にする。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
　【識別番号】　000003078
　【住所又は居所】　神奈川県川崎市幸区堀川町７２番地
　【氏名又は名称】　株式会社東芝
【代理人】　申請人
　【識別番号】　100058479
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　鈴江　武彦
【選任した代理人】
　【識別番号】　100084618
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　村松　貞男
【選任した代理人】
　【識別番号】　100068814
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　坪井　淳
【選任した代理人】
　【識別番号】　100092196
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　橋本　良郎
【選任した代理人】
　【識別番号】　100091351
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　中村　誠
【選任した代理人】

【識別番号】　100070437
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
【氏名又は名称】　河井　将次

出　願　人　履　歴　情　報

識別番号　　〔000003078〕

1．変更年月日　　1990年　8月22日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町72番地
氏　名　株式会社東芝